Express Mailing Label No. EL 571 476 692 US

PATENT APPLICATION
Docket No. 13768.164

UNITED STATES PATENT APPLICATION

of

Neil Fishman

and

Mike Kramer

for

CREDENTIAL AUTHENTICATION FOR MOBILE USERS

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

BACKGROUND OF THE INVENTION

1. The Field of the Invention

The present invention relates to authentication credentials. More specifically, the present invention relates to methods, systems, and computer program products for authenticating a mobile client that may have an input system optimized for numeric input.

2. Background and Related Art

Content stored on networks often is protected for a number of reasons. For example, content may include proprietary technology that provides a business with a competitive advantage. Many employers consider at least some portion of their personnel information private or confidential. It may be important to protect certain vital content, such as customer orders, from corruption or loss. Whether the motivation is to insure confidentiality or privacy, to prevent the corruption or loss of content, or to secure sensitive information, access to computer networks usually is governed through authentication credentials, such as a username and password for a particular system or domain.

However, authentication credentials for a computer network may be compromised in a number of ways, including brute force attacks, monitoring network traffic, and gaining access to third-party systems that store authentication credentials. In a brute force attack, a large number of potential authentication credentials, perhaps all possible combinations, are submitted to a computer network. For example, a four-digit PIN could be discovered by submitting the numbers from 0000 to 9999. Although submitting ten thousand numbers may seem like a significant task, for computers the imposition is minimal at best.

A common defense to brute force attacks is to increase the number of possibilities that must be submitted. Each added digit increases the number of potential selections by a

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111
T: 801.533.9800 F: 801.328.1707

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

factor of ten. If letters are available in addition to numbers, each character represents a factor of thirty-six. Including upper and lower case letter increases the weight of each character to sixty-two. For maximum protection, punctuation may be added to numbers and letters, arriving at a familiar one hundred and one possible choices for each character. (Typical English keyboards sold in the United States are described as 101 keyboards, indicating the number of printable characters that are supported.) Even if some characters are not allowed, with about one hundred options for each of four characters, the number of distinct combinations approaches 100 million, a significant improvement over the ten thousand combinations offered by a four-digit PIN.

Because arbitrary combinations of numbers, letters, and punctuation are difficult to remember, words, dates, acronyms, and the like, may help to keep authentication credentials familiar. Attackers exploit this weakness by employing a type of brute force attack, typically known as a dictionary attack. There is no need to try all combinations of letters or numbers; rather, only combinations that make sense as words, acronyms, or dates are submitted. Limiting the attack to a "dictionary" may reduce our 100 million improvement back to the range of ten or twenty thousand, and even less if only relatively common words are considered.

To reduce the threat posed by dictionary attacks, network administrators may impose policies regarding authentication credentials. For example, passwords may be required to include at least one upper case letter, at least one lower case letter, at least one number, and at least one punctuation character. In addition, a certain length may be mandated, such as five, six, seven, or eight characters. Because long passwords are more difficult to remember, specifying much more than eight characters may be counter productive because the passwords will be written down rather than memorized, allowing for authentication

credentials to be compromised if the written password is ever discovered. For example, an all too common occurrence in a financial context is storing a PIN with its corresponding charge or debit card. Any value to the PIN is all but lost if the PIN must be written to be remembered. Similar issues exist in other environments, particularly regarding access to computer networks.

Recently, there has been an increasing demand for access to computer networks, and the content they may offer, using mobile clients. Due to their convenient size and utility, telephones are among of the most widely-used mobile clients. However, some mobile clients, such as telephones, have input systems that are optimized for numeric input. While letters and punctuation may be available, it is often quite cumbersome for most users to enter any characters other than numbers. As described above, allowing authentication credentials that only contain digits makes a computer network vulnerable to brute force attacks.

Furthermore, third parties may be involved in providing mobile access to content. For example, telephones may connect to a wireless application protocol ("WAP") server in reaching a desired network or content server. In many circumstances, the WAP server and the network will be entirely unrelated. Businesses may be unwilling or unable to bear the expense of offering mobile access to their network, whereas telephone carriers will be able to use WAP servers as a revenue stream through increased airtime.

Intermediate servers represent a security risk, because wireless protocols may not provide for secure end-to-end connections. Secure connections may be limited to each hop, such as a secure connection between a telephone and a WAP server, and a secure connection between the WAP server and the network being accessed. As a result, the WAP server will contain unencrypted content. For example, the telephone may enter authentication

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

credentials that are encrypted during transit to the WAP server. The WAP server decrypts the authentication credentials and then re-encrypts the authentication credentials based on the secure protocol used in communicating with the network. If the WAP server is compromised, an attacker may be able to acquire authentication credentials that will allow access to any network that the mobile clients have accessed. Furthermore, to reduce the amount of information that must be remembered, mobile clients may use the same authentication credentials for other networks that do not provide mobile access, making those other networks vulnerable to attack as well.

Although it may be unlikely that an intermediate server will be compromised, the problem for the network is that the risk may be difficult to quantify. Security measures at the intermediate server are determined, implemented, monitored, and controlled, by whomever is responsible for the intermediate server. For some networks, the risk from numeric authentication credentials, coupled with uncertainty as to the extent of security provided by an intermediate server, will be too great, and mobile access will be prohibited.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

SUMMARY OF THE INVENTION

These and other problems are overcome by the present invention, which is directed toward authentication based on relatively weak credentials, such as passwords with few characters or passwords with limited selections for each character. For example, one client may have an input system optimized for numeric input and therefore use numeric only passwords, whereas another client may user relatively short passwords. In general, the present invention may be used to map one set of authentication credentials to another set of authentication credentials. A gateway receives authentication credentials from the client and uses an authentication filter to map the authentication credentials according to pre-established criteria. The authentication filter may change the domain name, the username, or both. For example, one domain name may be substituted for another, or a suffix may be added to the username. Then the mapped authentication credentials are sent to the network that includes the content server being accessed. Any access privileges granted to the client are based on the mapped authentication credentials.

The gateway allows for authentication credentials that are specific to client access through the gateway, without disclosing information about the network to which clients connect. If a client's credentials are compromised, attempts to authenticate with the credentials that do not involve the gateway will fail because the specified domain name, username, or both, do not exist on the network. Furthermore, the gateway may be configured to accept connections only from known third party servers. As a result, any authentication credentials that may be discovered by an attacker are limited to use in a gateway context.

By defining authentication credentials that are specific to client access through the gateway, network administrators are able to balance an appropriate level of access

permissions with the increased level of risk that results from weak credentials, such as numeric passwords. Rather than granting the same level of access that a user would enjoy using other authentication credentials, such as when authenticating with an office computer over an internal network connection, gateway authentication credentials can be restricted to insure minimal exposure if compromised. For example, gateway authentication credentials may be limited to the network resources of a single user, such as the user's email account, a default login directory, etc., whereas other authentication credentials might allow the user access to a large number of network resources that are ordinarily shared among a number of users, including servers, directories, databases, etc.

The gateway also facilitates management of gateway authentication credentials. The domain names and/or usernames may be updated without imposing hardship on the clients. For example, if it appears that a domain has been compromised, a new domain may be created or new accounts in a domain may be created and the gateway configured accordingly. Gateway authentication credentials may be associated with other authentication credentials to identify potential resources that clients may access, with specific access permissions granted as appropriate. In other words, gateway authentication credentials would not grant permissions greater than those provided for in the other authentication credentials.

A trust relationship may be established between various authentication credentials and corresponding domains. The trust relationship defines specific areas of trust. For example, one domain may trust the authentication credentials in another domain for delegate access privileges, but not for other, more sensitive privileges, such as administrator privileges. Defining a trust relationship offers an additional level of control over mobile

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

access privileges because it prevents mobile authentication credentials from superceding other authentication qualifications.

Additional features and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by the practice of the invention. The features and advantages of the invention may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. These and other features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth hereinafter.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

BRIEF DESCRIPTION OF THE DRAWINGS

In order to describe the manner in which the above-recited and other advantages and features of the invention can be obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered as limiting its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 illustrates an exemplary system that provides a suitable operating environment for the present invention;

Figure 2 is a block diagram showing a network with separate domains for mobile and other authentication credentials;

Figure 3 is a block diagram showing a network with a single domain for mobile and other authentication credentials; and

Figure 4 illustrates an exemplary method for authenticating a mobile client through a mobile gateway.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

DETAILED DESCRIPTION OF THE INVENTION

The present invention extends to methods, systems, and computer program products for authenticating clients. A gateway maps authentication credentials received from a client and sends the mapped authentication credentials to a network that includes the resources the client desires to access. Authentication credentials identify a particular client and determine the resources the client is authorized to access, including the types of access permitted.

Authentication credentials often include a username and password for one or more domains. Other types of information, including biometric attributes (e.g., fingerprints) and hardware keys (e.g., smartcards), may be used as well. The present invention is not limited to any particular type of authentication credentials. Authentication credentials ordinarily apply to a group or collection of one or more resources, often referred to as a domain. Domains facilitate resource administration by allowing resources to be managed as a single unit, with common rules and procedures. More generally, the term "domain" describes a logical grouping of resources, wherein the grouping may be independent of how resources are interconnected. A single network may have one or more domains and a single domain may include one or more networks.

At times, authentication credentials may be described as weak or short. As used in this application, however, weak and short should be interpreted as a comparative, rather than absolute, terms. Weak and/or short authentication credentials are weak and/or short only in that stronger and/or longer authentication credentials are possible and may be desirable. For example, a four-digit password is weak and short in comparison to a five-digit password. Similarly, a five-digit password is weak, although not short, in comparison to a five-character alphanumeric password. In its most general sense, the present invention involves substituting one set of authentication credentials for another. The specific

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

examples discussed below merely identify exemplary environments or embodiments for practicing the present invention and should not be interpreted as necessarily limiting its scope.

The term "client" may be used to describe individuals, devices, computers, systems, etc., either alone or in combination, that access computer resources. The term "server" describes a provider of computer resources, and likewise includes devices, computers, systems, etc. Depending on the circumstances, a server in one setting may be a client in another, and likewise, a client in one setting may be a server at other times. The term network describes interconnected resources, and encompasses a wide range of configurations, including a single resource, such as a computer, storage system, printer, file server, etc., that allows connections with clients and/or any other resource.

Each of the foregoing terms should be accorded the widest possible interpretation. Those of skill in the art may recognize that, in a particular context, certain terms may acquire a more specific or alternate meaning. It should be noted, therefore, that the following detailed description is offered to present exemplary implementations and is not intended to limit the scope of the present invention. The embodiments of the present invention may comprise a special purpose or general purpose computer including various computer hardware, as discussed in greater detail below.

Embodiments within the scope of the present invention also include computer-readable media for carrying or having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media which can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111
T 801 533 9800 F 801 328 1707

other medium which can be used to carry or store desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a computer-readable medium. Thus, any such a connection is properly termed a computer-readable medium. Combinations of the above should also be included within the scope of computer-readable media. Computer-executable instructions comprise, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions.

Figure 1 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the invention may be implemented. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by computers in network environments. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures, and program modules represent examples of the program code means for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represent examples of corresponding acts for implementing the functions described in such steps.

Those skilled in the art will appreciate that the invention may be practiced in network computing environments with many types of computer system configurations,

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

including personal computers, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by local and remote processing devices that are linked (either by hardwired links, wireless links, or by a combination of hardwired or wireless links) through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

With reference to Figure 1, an exemplary system for implementing the invention includes a general purpose computing device in the form of a conventional computer 20, including a processing unit 21, a system memory 22, and a system bus 23 that couples various system components including the system memory 22 to the processing unit 21. The system bus 23 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory includes read only memory (ROM) 24 and random access memory (RAM) 25. A basic input/output system (BIOS) 26, containing the basic routines that help transfer information between elements within the computer 20, such as during start-up, may be stored in ROM 24.

The computer 20 may also include a magnetic hard disk drive 27 for reading from and writing to a magnetic hard disk 39, a magnetic disk drive 28 for reading from or writing to a removable magnetic disk 29, and an optical disk drive 30 for reading from or writing to removable optical disk 31 such as a CD-ROM or other optical media. The magnetic hard disk drive 27, magnetic disk drive 28, and optical disk drive 30 are connected to the system bus 23 by a hard disk drive interface 32, a magnetic disk drive-interface 33, and an optical drive interface 34, respectively. The drives and their associated computer-readable media

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

provide nonvolatile storage of computer-executable instructions, data structures, program modules and other data for the computer 20. Although the exemplary environment described herein employs a magnetic hard disk 39, a removable magnetic disk 29 and a removable optical disk 31, other types of computer readable media for storing data can be used, including magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, RAMs, ROMs, and the like.

Program code means comprising one or more program modules may be stored on the hard disk 39, magnetic disk 29, optical disk 31, ROM 24 or RAM 25, including an operating system 35, one or more application programs 36, other program modules 37, and program data 38. A user may enter commands and information into the computer 20 through keyboard 40, pointing device 42, or other input devices (not shown), such as a microphone, joy stick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 21 through a serial port interface 46 coupled to system bus 23. Alternatively, the input devices may be connected by other interfaces, such as a parallel port, a game port or a universal serial bus (USB). A monitor 47 or another display device is also connected to system bus 23 via an interface, such as video adapter 48. In addition to the monitor, personal computers typically include other peripheral output devices (not shown), such as speakers and printers.

The computer 20 may operate in a networked environment using logical connections to one or more remote computers, such as remote computers 49a and 49b. Remote computers 49a and 49b may each be another personal computer, a server, a router, a network PC, a peer device or other common network node, and typically include many or all of the elements described above relative to the computer 20, although only memory storage devices 50a and 50b and their associated application programs 36a and 36b have been

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

illustrated in Figure 1. The logical connections depicted in Figure 1 include a local area network (LAN) 51 and a wide area network (WAN) 52 that are presented here by way of example and not limitation. Such networking environments are commonplace in office-wide or enterprise-wide computer networks, intranets and the Internet.

When used in a LAN networking environment, the computer 20 is connected to the local network 51 through a network interface or adapter 53. When used in a WAN networking environment, the computer 20 may include a modem 54, a wireless link, or other means for establishing communications over the wide area network 52, such as the Internet. The modem 54, which may be internal or external, is connected to the system bus 23 via the serial port interface 46. In a networked environment, program modules depicted relative to the computer 20, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing communications over wide area network 52 may be used.

The block diagram of Figure 2 shows network 210 with separate domains, mobile domain 240 and other domain(s) 230, for managing mobile and other authentication credentials, respectively. Mobile domain 240 may be recognized generally by network 210 or may be used only in providing access to content server 220. Other domain(s) 230 includes username 232, identifying Neil as a user, with a password 234 of A1(b)c5. (Note that the use of upper and lower case characters, numbers, and punctuation, provides a significant defense against brute force attacks.) Mobile domain 240 includes username 242, identifying Neil-m as a user, with a numeric password 244 of 1234. As indicated by references 212 and 214, both Neil and Neil-m have access permissions for content server 220.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

Because mobile domain 240 is separate from other domain(s) 230, it is not necessary for username 242 and username 232 to be different. Either separate usernames or separate domain names is sufficient for providing authentication credentials that are specific to a mobile client. In practice, administration of the two domains may be simplified if usernames are shared. For example, a trust relationship may be established between the two domains. The extent of the trust relationship between the domains depends on the circumstances of a particular implementation, but the mobile domains would be trusted with respect to some minimal level of access permissions, such as delegate permissions in an email context. The different usernames, however, aid below in distinguishing between comments referring to other domain(s) 230 and comments that refer to mobile domain 240. The distinct usernames, Neil and Neil-m, therefore, will be retained throughout the remaining discussion of Figure 2 for the sake of clarity. Note that Figure 3 focuses attention on the use of a single domain with different usernames.

To account for the increased risk associated with mobile clients, the access permissions granted through mobile domain 240 are limited as compared to those granted by other domain(s) 230. For example, if content server 220 provides email resources, Neil may have all access rights for a particular email account, whereas Neil-m may be granted only certain delegate access privileges. Furthermore, Neil also may have access privileges to other resources that are part of other domain(s) 230, whereas Neil-m's access privileges extend only to content server 220.

Access privileges may apply to one or multiple clients. For example, the owner or administrator of a resource may have one set of access privileges, certain groupings or domains may have another set of access privileges, and all others may have a default set of access privileges. Those of skill in the art will recognize that a variety of schemes for

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

specifying access privileges exist and that others may be developed in the future. It should be noted that the present invention is not limited to any particular form of access privileges. Rather, the present invention recognizes that it may be desirable to provide separate access privileges for mobile clients, and provides the relevant technology for doing so, independent of the underlying implementation access privileges.

If the authentication credentials associated with Neil-m were compromised, only the resources available to a single mobile client would be accessible. For email resources, this probably will include only the mobile client's mailbox. In contrast, compromising the authentication credentials associated with Neil, are likely to yield much wider access privileges to resources of network 210 that are probably shared by various clients.

Alternatively mobile domain 240 may be a separately administered credential database that is only used in providing access to content server 220. In this case, mobile domain 240 is not a domain in the same sense that other domain(s) 230 is a domain. The separately administered credential database could not be used for direct access of resources that are part of network 210. Rather, content server 220 may be configured to verify authentication credentials included within this credential database. Once verified, a shared account in a domain, such as other domain(s) 230, would be used in accessing content server 220. As above, if the authentication credentials for Neil-m were compromised, only the resources available to a single mobile client would be at risk, such as the client's mailbox. However, if the shared account were compromised, resources associated with all mobile clients would be at risk.

Turning now to the flow of authentication credentials from any of various mobile clients to network 210, phone 280 provides authentication credentials to WAP server 270 over connection 296. Although a textual username (Neil) is shown in Figure 2, the

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

username is ordinarily stored at the phone so it does not need to be entered each time a request for content is made. Connection 296 may be encrypted, using a protocol such as wireless transport layer security ("WTLS"), to protect content exchanged between phone 280 and WAP server 270. WAP server 270 decrypts the authentication credentials and sends them to mobile gateway 250 over connection 294. Like connection 296, connection 294 may encrypt the authentication credentials using a protocol such as secure sockets layer ("SSL"). Typically, WAP server 270 operates as a protocol translator between the wireless protocols of mobile clients and the wireline protocols used in communicating with mobile gateway 250. The authentication credentials are subject to attack at the WAP server because, at least for a time, they are unencrypted. Furthermore, because the authentication credentials are likely to include relative short numeric portions, such as a numeric password or PIN, the authentication credentials are vulnerable to brute force attacks.

Mobile gateway 250 includes an authentication filter 260 that is used in mapping received authentication credentials. Authentication filter 260 includes two components, domain identifier 266 and username modifier 262. The domain identifier 266 specifies the domain that network 210 will use in processing authentication credentials. In Figure 2, the domain identifier is Mobile. Changing a domain name in accordance with domain identifier 266 includes substituting one domain for another (replacing a domain specified by a mobile client with domain identifier 266), altering a domain name (making a change to a domain specified by a mobile client), and adding a domain where none was specified (adding domain identifier 266 where a mobile client did not specify a domain), etc. The username modifier 262 includes a username box 262a and a suffix 262b. Username box 262a is simply a placeholder for all usernames, whereas the mobile gateway adds suffix

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

262b to usernames. Mobile gateway 250 sends network 210 mapped authentication credentials over connection 292, using encryption as appropriate.

Network 210 processes the authentication credentials it receives as described above. Note that mobile gateway 250 identifies both a separate mobile domain 240 and adds a username suffix. If the username Neil, and password 1234 are entered at phone 280, mobile gateway changes the username to Neil-m and sends the authentication credentials to mobile domain 240 for processing. Because a username Neil-m, with a password of 1234, exists in mobile domain 240, phone 280 will be granted the access privileges that are associated with Neil-m. Ordinarily, only a separate mobile domain, such as mobile domain 240, or a username suffix is needed to provide authentication credentials that are specific to a mobile client.

The block diagram of Figure 3 shows a network with a single domain, corporate domain 330, for both mobile and other authentication credentials. A username 332 of Mike with a password 334 of X9(y)z3 is defined in corporate domain 330 for determining access privileges to the resources, such as content server 320, of network 310. A mobile client, with a username 342 of Mike-m and a password 344 of 5678 is also defined in corporate domain 330. Note that the present invention does not require that any particular suffix be added to usernames. Furthermore, the present invention does not necessarily require changing usernames by adding a suffix. Usernames may be changed by adding a prefix, inserting characters into the middle of a username, substituting all or a portion of a username for another portion or username, deleting characters from a username, etc.

Similar to the description with reference to Figure 2, and turning now to the flow of authentication credentials from any of various mobile clients to network 310, phone 380 provides authentication credentials to WAP server 370 over connection 396, using WTLS.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

WAP server 370 decrypts the authentication credentials received over connection 396 and re-encrypts the authentication credentials for SSL connection 394. At mobile gateway 350, authentication filter 360 adds suffix 362b to usernames 362a, as indicated by reference 362. Mobile gateway 350 sets the applicable domain 366 for the received authentication credentials to Corporate.

If the username Mike, and password 5678 are entered at phone 380, mobile gateway changes the username to Mike-m and sends the authentication credentials to corporate domain 330 for processing. Because a username Mike-m, with a password of 5678, exists in corporate domain 330, phone 380 will be granted the access privileges that are associated with Mike-m. Here, only a single domain, such as corporate domain 330, is needed to provide authentication credentials that are specific to a mobile client.

One drawback to the single domain implementation is that policies and procedures for authentication credentials are often set on a domain basis. That is, corporate domain 330 may be set to require at least one upper case letter, at least one lower case letter, a number, and a punctuation character, in all passwords. By having Mike-m in corporate domain 330, password 344 would be subject to these requirements, and therefore, an all-numeric password, such as 5678, may not be allowed.

It should also be noted that authentication filter 360 is capable of making whatever changes to authentication credentials that are appropriate for the type and format of authentication credentials implemented by network 310, content server 320, and/or corporate domain 330. As reference 312 shows, content server 320 depends on corporate domain 330 for determining access privileges. A particular implementation of authentication credentials, however, is not necessarily limited by the present invention. Any changes that mobile gateway 350 makes need only be proper for the authentication

credentials that are expected by network 310, content server 320, and/or corporate domain 330. Where a separately administered authentication credential database provides access to resources, the mapping performed by a mobile gateway may be specific to the separate credential database, even though those mappings would not be appropriate for network 310 or any associated domains.

Turning now to Figure 4, an exemplary method for authenticating a mobile client through a mobile gateway is illustrated. A step for altering (410) authentication credentials may include the acts of defining (412) an authentication filter and mapping (414) any received authentication credentials. Mapping may include changing the domain name, username, or otherwise modifying the authentication credentials. One domain name may be substituted for another and usernames may have a suffix added.

A step for identifying (420) a mobile client may include the acts of receiving (422) authentication credentials from a mobile client and sending (424) the mapped authentication credentials to a network providing the resources that will be requested by the mobile client. The steps of altering (410) authentication credentials and identify (420) a mobile client are intertwined to indicate that the acts associated with the steps are not necessarily performed in any particular order. A step for accessing (430) content provided by the network may include the acts of receiving (432) a request for content, sending (434) the request to the network, receiving (436) the requested content, and sending (438) the requested content to the mobile client.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured by United States Letters Patent is:

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111